A duality relation connecting different quantum generalizations of the conditional Rényi entropy

Marco Tomamichel
Centre for Quantum Technologies,
National University of Singapore
Email: cqtmarco@nus.edu.sg

Mario Berta
Institute for Theoretical Physics,
ETH Zurich,
Email: berta@phys.ethz.ch

Masahito Hayashi
Graduate School of Mathematics,
Nagoya University, and
Centre for Quantum Technologies,
National University of Singapore
Email: masahito@math.nagoya-u.ac.jp

***Abstract*—Recently a new quantum generalization of the Rényi divergence and the corresponding conditional Rényi entropies was proposed. Here we report on a surprising relation between conditional Rényi entropies based on this new generalization and conditional Rényi entropies based on the quantum relative Rényi entropy that was used in previous literature. This generalizes the well-known duality relation $H(A|B)+H(A|C)=0$ for tripartite pure states to Rényi entropies of two different kinds.**

As a direct application, we prove a collection of inequalities that relate different conditional Rényi entropies.

I. Introduction

Recently, there has been renewed interest in finding suitable quantum generalizations of Rényi's [33] entropies and divergences. This is due to the fact that Rényi entropies and divergences have a wide range of applications in classical information theory and cryptography, see, e.g. [11].

We will review some of the recent progress here, but refer the reader to [29] for a more in-depth discussion. For our purposes, a quantum system is modeled by a finite dimensional Hilbert space. We denote by $\mathcal{P}$ the set of positive semi-definite operators on that Hilbert space, and by $\mathcal{S}$ the subset of density operators with unit trace.

The following natural quantum generalization of the Rényi divergence has been widely used and has found operational significance, for example, as a cut-off rate in quantum hypothesis testing [26] (see also [30], [31]). It is usually referred to as *quantum Rényi relative entropy* and for all $\alpha \in (0,1)\cup(1,\infty)$ defined as

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log\operatorname{tr}\left\{\rho^\alpha\sigma^{1-\alpha}\right\} \tag{1}$$

for arbitrary $\rho \in \mathcal{S}$, $\sigma \in \mathcal{P}$ that satisfy $\rho \ll \sigma$.[1]

While this definition has proven useful in many applications, it has a major drawback in that it does not satisfy the data-processing inequality (DPI) for $\alpha > 2$. The DPI states that the quantum Rényi relative entropy is contractive under application of a quantum channel, i.e., $D_\alpha\big(\mathcal{E}[\rho]\big\|\mathcal{E}[\sigma]\big) \leq D_\alpha(\rho\|\sigma)$ for any completely positive trace-preserving map $\mathcal{E}$. Intuitively, this property is very desirable since we want to think of the divergence as a measure of how well ρ can be distinguished from σ, and this can only get more difficult after a channel is applied.

Recently, an alternative quantum generalization of the Rényi divergence has been investigated [28], [29], [38] (see also [35]). It is referred to as *quantum Rényi divergence*,[2] and defined as

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log\operatorname{tr}\left\{\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right\} \tag{2}$$

under the same constraints. The quantum Rényi divergence has found operational significance in the converse part of quantum hypothesis testing [27]. As such, it satisfies the DPI for all $\alpha \geq \frac{1}{2}$ as was shown by Frank and Lieb [13] and independently by Beigi [6] for $\alpha > 1$. (See also earlier work [28], [29] where a different proof is given for $\alpha \in (1,2]$ and [27] for an alternative, more operational proof.) Furthermore, the quantum Rényi divergence has already proven an indispensable tool, for example in the study of strong converse capacities of quantum channels [15], [38]

The definitions, (1) and (2), are in general different but coincide when ρ and σ commute. For $\alpha \in \{0,1,\infty\}$, we define $D_\alpha(\rho\|\sigma)$ and $\widetilde{D}_\alpha(\rho\|\sigma)$ as the corresponding limit. In the limit $\alpha \to 1$ both expressions converge to the quantum relative entropy [28], [29], [38], namely

$$D_1(\rho\|\sigma) = \widetilde{D}_1(\rho\|\sigma) = D(\rho\|\sigma) := \operatorname{tr}\left\{\rho(\log\rho - \log\sigma)\right\}.$$

It has been observed [12], [38] that the relation

$$D_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\rho\|\sigma) \tag{3}$$

follows from the Araki-Lieb-Thirring trace inequality [1], [24]. Furthermore, $\alpha \mapsto D_\alpha(\rho\|\sigma)$ and $\alpha \mapsto \widetilde{D}_\alpha(\rho\|\sigma)$ are monotonically increasing functions. For the latter quantity, this was shown in [29] and independently in [6].

Finally, very recently Audenaert and Datta [4] defined a more general two parameter family of *α-z-relative Rényi entropies* of the form

$$D_{\alpha,z}(\rho\|\sigma) := \frac{1}{\alpha-1}\log\operatorname{tr}\left\{\left(\rho^{\frac{\alpha}{z}}\sigma^{\frac{1-\alpha}{z}}\right)^z\right\},$$

[1]The notation $\rho \ll \sigma$ means that σ dominates ρ, i.e. the kernel of σ lies inside the kernel of ρ.

[2]It is also called sandwiched Rényi relative entropy in [38].

and explored some of its properties. We clearly have $D_\alpha \equiv D_{\alpha,1}$ and $\widetilde{D}_\alpha \equiv D_{\alpha,\alpha}$.

II. Quantum Conditional Rényi Entropies

We will in the following consider disjoint quantum systems, denoted by capital letters A, B and C. The sets $\mathcal{P}(A)$ and $\mathcal{S}(A)$ take on the expected meaning.

The conditional von Neumann entropy can be conveniently expressed in terms of the quantum relative entropy as follows. For a bipartite state $\rho_{AB} \in \mathcal{S}(AB)$, we define

$$\begin{aligned} H(A|B)_\rho &:= H(\rho_{AB}) - H(\rho_B) && (4)\\ &= -D(\rho_{AB} \| 1_A \otimes \rho_B) && (5)\\ &= \sup_{\sigma_B \in \mathcal{S}(B)} -D(\rho_{AB} \| 1_A \otimes \sigma_B), && (6)\end{aligned}$$

where $H(\rho) := -\operatorname{tr}\{\rho \log \rho\}$ is the usual von Neumann entropy. The last equality can be verified using the relation $D(\rho_{AB} \| 1_A \otimes \sigma_B) = D(\rho_{AB} \| 1_A \otimes \rho_B) + D(\rho_B \| \sigma_B)$ together with the fact that $D(\cdot\|\cdot)$ is positive definite.

In the case of Rényi entropies, it is not immediate which expression — (4), (5) or (6) — should be used to define the conditional Rényi entropies. It has been found in the study of the classical special case (see, e.g. [22] for an overview) that generalizations based on (4) have severe limitations, for example they cannot be expected to satisfy a DPI. On the other hand, definitions based on the underlying divergence, as in (5) or (6), have proven to be very fruitful and lead to quantities with operational significance. Together with the two proposed quantum generalizations of the Rényi divergence in (1) and (2), this leads to a total of four different candidates for conditional Rényi entropies. For $\alpha \geq 0$ and $\rho_{AB} \in \mathcal{S}(AB)$, we define

$$\begin{aligned} H_\alpha^\downarrow(A|B)_\rho &:= -D_\alpha(\rho_{AB} \| 1_A \otimes \rho_B), && (7)\\ H_\alpha^\uparrow(A|B)_\rho &:= \sup_{\sigma_B \in \mathcal{S}(B)} -D_\alpha(\rho_{AB} \| 1_A \otimes \sigma_B), && (8)\\ \widetilde{H}_\alpha^\downarrow(A|B)_\rho &:= -\widetilde{D}_\alpha(\rho_{AB} \| 1_A \otimes \rho_B), \quad \text{and} && (9)\\ \widetilde{H}_\alpha^\uparrow(A|B)_\rho &:= \sup_{\sigma_B \in \mathcal{S}(B)} -\widetilde{D}_\alpha(\rho_{AB} \| 1_A \otimes \sigma_B). && (10)\end{aligned}$$

The fully quantum entropy $H_\alpha^\downarrow$ has first been studied in [36]. For the classical and classical-quantum special case this quantity gives a generalization of the leftover hashing lemma [7] for the modified mutual information to Rényi entropies with $\alpha \neq 2$ [17], [18].

The classical version of $H_\alpha^\uparrow$ was introduced by Arimoto for an evaluation of the guessing probability [2]. We note that he used another but equivalent expression for $H_\alpha^\uparrow$ that we later explain in Lemma 1. Then, Gallager used $H_\alpha^\uparrow$ (again in the form of Lemma 1) to upper bound the decoding error probability of a random coding scheme for data compression with side-information [14] (see also [39]). The classical and classical-quantum special cases of $H_\alpha^\uparrow$ were, for example, also investigated in [18], [20] and realize another type of a generalization of the leftover hashing lemma for the L_1-distinguishability in the study of randomness extraction to Rényi entropies with $\alpha \neq 2$.

It follows immediately from the definition and the corresponding property of D_α that these two entropies satisfy a data-processing inequality. Namely for any quantum operation $\mathcal{E}_{B\to B'}$ with $\tau_{AB'} = \mathcal{E}_{B\to B'}[\rho_{AB}]$ and any $\alpha \in [0, 2]$, we have

$$H_\alpha^\downarrow(A|B)_\rho \leq H_\alpha^\downarrow(A|B')_\tau \quad \text{and} \quad H_\alpha^\uparrow(A|B)_\rho \leq H_\alpha^\uparrow(A|B')_\tau.$$

The conditional entropy $\widetilde{H}_\alpha^\uparrow$ was investigated in [29] and $\widetilde{H}_\alpha^\downarrow$ is first considered in this paper. Since the relative entropies $\widetilde{D}_\alpha$ and D_α are identical for commuting operators, we note that $\widetilde{H}_\alpha^\uparrow = H_\alpha^\uparrow$ as well as $\widetilde{H}_\alpha^\downarrow = H_\alpha^\downarrow$ for classical distributions. Again, both quantum generalizations satisfy the above data-processing inequality but this time for $\alpha \geq \frac{1}{2}$.

Furthermore, it is easy to verify that all entropies considered are invariant under applications of local isometries on either the A or B systems. Also note that the optimization over σ_B can always be restricted to $\sigma_B \gg \rho_B$ for $\alpha > 1$. Moreover, inheriting these properties from the corresponding divergences, all entropies are monotonically decreasing functions of α.

Note that we use up and down arrows to express the trivial observation that $H_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho$ and $\widetilde{H}_\alpha^\uparrow(A|B)_\rho \geq \widetilde{H}_\alpha^\downarrow(A|B)_\rho$ by definition. More interestingly, (3) gives us the additional relations $\widetilde{H}_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\uparrow(A|B)_\rho$ and $\widetilde{H}_\alpha^\downarrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho$. These relations are summarized in Figure 1 and will be of value later.

For $\alpha = 1$, all definitions coincide with the usual conditional von Neumann entropy, Eq. (5). For $\alpha = \infty$, two quantum generalizations of the conditional min-entropy emerge, which both have been studied by Renner [32]. Namely,[3]

$$\begin{aligned} \widetilde{H}_\infty^\downarrow(A|B)_\rho &= \sup\left\{\lambda \in \mathbb{R} \,\middle|\, \rho_{AB} \leq 2^{-\lambda} 1_A \otimes \rho_B\right\}, && (11)\\ \widetilde{H}_\infty^\uparrow(A|B)_\rho &= \sup\left\{\lambda \in \mathbb{R} \,\middle|\, \rho_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B,\right. \\ &\qquad\qquad \left. \sigma_B \in \mathcal{S}(B)\right\}. && (12)\end{aligned}$$

For $\alpha = 2$, we find a quantum generalization of the conditional collision entropy as introduced by Renner [32]:

$$\widetilde{H}_2^\downarrow(A|B)_\rho = -\log \operatorname{tr}\left\{\left(\rho_{AB}\left(1_A \otimes \rho_B^{-\frac{1}{2}}\right)\right)^2\right\}. \qquad (13)$$

For $\alpha = \frac{1}{2}$, we find the quantum conditional max-entropy first studied by König *et al.* [23],[4]

$$\widetilde{H}_{1/2}^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}(B)} \log F(\rho_{AB}, 1_A \otimes \sigma_B), \qquad (14)$$

where $F(\cdot,\cdot)$ denotes Uhlmann's fidelity. For $\alpha = 0$, we find a quantum conditional generalization of the Hartley entropy [16] that was initially considered by Renner [32],

$$H_0^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}(B)} \log \operatorname{tr}\{\Pi_{\rho_{AB}}\, 1_A \otimes \sigma_B\}, \qquad (15)$$

where Π_ρ denotes the projector onto the support of ρ.

[3] The notation $H_{\min}(A|B)_{\rho|\rho} \equiv \widetilde{H}_\infty^\downarrow(A|B)_\rho$ and $H_{\min}(A|B)_\rho \equiv \widetilde{H}_\infty^\uparrow(A|B)_\rho$ is widely used. However, we prefer our notation as it makes our exposition in this manuscript clearer.

[4] The notation $H_{\max}(A|B)_\rho \equiv \widetilde{H}_{1/2}^\uparrow(A|B)_\rho$ is often used.

$$\begin{tikzcd}
H_\alpha^{\uparrow}(A|B)_\rho \arrow[d] & \widetilde{H}_\alpha^{\uparrow}(A|B)_\rho \arrow[l] \arrow[d] \arrow[dl] \\
H_\alpha^{\downarrow}(A|B)_\rho & \widetilde{H}_\alpha^{\downarrow}(A|B)_\rho \arrow[l]
\end{tikzcd}$$

Fig. 1. Overview of the different conditional entropies used in this paper. Arrows indicate that one entropy is larger or equal to the other for all states $\rho_{AB} \in \mathcal{S}(AB)$ and all $\alpha \geq 0$.

III. Duality Relations

It is well known that, for any tripartite pure state ρ_{ABC}, the relation

$$H(A|B)_\rho + H(A|C)_\rho = 0 \tag{16}$$

holds. We call this a *duality relation* for the conditional entropy. To see this, simply write $H(A|B)_\rho = H(\rho_{AB}) - H(\rho_B)$ and $H(A|C)_\rho = H(\rho_{AC}) - H(\rho_C)$ and note that the spectra of ρ_{AB} and ρ_C as well as the spectra of ρ_B and ρ_{AC} agree. The significance of this relation is manifold — for example it turns out to be useful in cryptography where the entropy of an adversarial party, let us say C, can be estimated using local state tomography by two honest parties, A and B. In the following, we are interested to see if such relations hold more generally for conditional Rényi entropies.

It was shown in [36, Lm. 6] that $H_\alpha^{\downarrow}$ indeed satisfies a duality relation, namely

$$H_\alpha^{\downarrow}(A|B)_\rho + H_\beta^{\downarrow}(A|C)_\rho = 0 \quad \text{when } \alpha + \beta = 2,\ \alpha, \beta \geq 0\,.$$

Note that the map $\alpha \mapsto \beta = 2 - \alpha$ maps the interval $[0, 2]$, where data-processing holds, onto itself. This is not surprising. Indeed, consider the Stinespring dilation $\mathcal{U}_{B \to B'B''}$ of a quantum channel $\mathcal{E}_{B \to B'}$. Then, for ρ_{ABC} pure, $\tau_{AB'B''C} = \mathcal{U}_{B\to B'B''}[\rho_{ABC}]$ is also pure and the above duality relation implies that

$$H_\alpha^{\downarrow}(A|B)_\rho \leq H_\alpha^{\downarrow}(A|B')_\tau \iff H_\beta^{\downarrow}(A|C)_\rho \geq H_\beta^{\downarrow}(A|B''C)_\tau\,.$$

Hence, data-processing for α holds if and only if data-processing for β holds.

A similar relation has recently been discovered for $\widetilde{H}_\alpha^{\uparrow}$ in [29] and independently in [6]. There, it is shown that

$$\widetilde{H}_\alpha^{\uparrow}(A|B)_\rho + \widetilde{H}_\beta^{\uparrow}(A|C)_\rho = 0 \quad \text{when } \frac{1}{\alpha} + \frac{1}{\beta} = 2,\ \alpha, \beta \geq \frac{1}{2}\,.$$

As expected, the map $\alpha \mapsto \beta = \frac{\alpha}{2\alpha - 1}$ maps the interval $[\frac{1}{2}, \infty]$, where data-processing holds, onto itself.

The purpose of the following is thus to show if a similar relation holds for the remaining two candidates, $H_\alpha^{\uparrow}$ and $\widetilde{H}_\alpha^{\downarrow}$. First, we find the following alternative expression for $H_\alpha^{\uparrow}$ by determining the optimal σ_B in the definition (8).

Lemma 1. *Let $\alpha \in (0,1) \cup (1, \infty)$ and $\rho_{AB} \in \mathcal{S}(AB)$. Then,*

$$H_\alpha^{\uparrow}(A|B)_\rho = \frac{\alpha}{1-\alpha} \log \operatorname{tr} \Big\{ \big(\operatorname{tr}_A \{\rho_{AB}^\alpha\} \big)^{\frac{1}{\alpha}} \Big\}. \tag{17}$$

This generalizes a result by one of the present authors [18, Lm. 7].

Proof. Recall the definition

$$\begin{aligned} H_\alpha^{\uparrow}(A|B)_\rho &= \sup_{\sigma_B \in \mathcal{S}(B)} \frac{1}{1-\alpha} \log \operatorname{tr} \left\{ \rho_{AB}^\alpha\, 1_A \otimes \sigma_B^{1-\alpha} \right\} \\ &= \sup_{\sigma_B \in \mathcal{S}(B)} \frac{1}{1-\alpha} \log \operatorname{tr} \left\{ \operatorname{tr}_A \{\rho_{AB}^\alpha\} \sigma_B^{1-\alpha} \right\}. \end{aligned}$$

This can immediately be lower bounded by the expression in (17) by substituting

$$\sigma_B^* = \frac{\big(\operatorname{tr}_A\{\rho_{AB}^\alpha\}\big)^{\frac{1}{\alpha}}}{\operatorname{tr}\Big\{\big(\operatorname{tr}_A\{\rho_{AB}^\alpha\}\big)^{\frac{1}{\alpha}}\Big\}}$$

for σ_B. It remains to show that this choice is optimal. We employ the following Hölder and reverse Hölder inequalities (cf. Lemma 5 in Appendix A). For any $A, B \geq 0$, the Hölder inequality states that

$$\operatorname{tr}\{AB\} \leq \big(\operatorname{tr}\{A^p\}\big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \qquad \text{for all } p, q > 1 \text{ s.t. } \frac{1}{p} + \frac{1}{q} = 1. \tag{18}$$

Furthermore, if $B \gg A$, we employ a reverse Hölder inequality which states that

$$\operatorname{tr}\{AB\} \geq \big(\operatorname{tr}\{A^p\}\big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \qquad \text{for all } q < 0 < p < 1 \text{ s.t. } \frac{1}{p} + \frac{1}{q} = 1,\,. \tag{19}$$

For $\alpha < 1$, we employ (18) for $p = \frac{1}{\alpha}$, $q = \frac{1}{1-\alpha}$, $A = \operatorname{tr}_A\{\rho_{AB}^\alpha\}$ and $B = \sigma_B^{1-\alpha}$ to find

$$\operatorname{tr}\left\{ \operatorname{tr}_A\{\rho_{AB}^\alpha\}\sigma_B^{1-\alpha} \right\} \leq \Big(\operatorname{tr}\Big\{ \big(\operatorname{tr}_A\{\rho_{AB}^\alpha\}\big)^{\frac{1}{\alpha}} \Big\} \Big)^\alpha \big(\operatorname{tr}\{\sigma_B\}\big)^{1-\alpha},$$

which yields the desired upper bound since $\operatorname{tr}\{\sigma_B\} = 1$. For $\alpha > 1$, we instead use (19). This leads us to (17) upon the same substitutions, concluding the proof. $\square$

An alternative proof also follows by a quantum generalization of Sibson's identity, see, e.g. [34].

This allows us to show our main result.

Theorem 2. *Let $\alpha, \beta \in (0,1) \cup (1,\infty)$ with $\alpha \cdot \beta = 1$ and let $\rho_{ABC} \in \mathcal{S}(ABC)$ be pure. Then,*

$$H_\alpha^{\uparrow}(A|B)_\rho + \widetilde{H}_\beta^{\downarrow}(A|C)_\rho = 0.$$

Proof. After substituting $\beta = \frac{1}{\alpha}$ and employing Lemma 1, it remains to show that

$$\begin{aligned} &\frac{\alpha}{1-\alpha} \log \operatorname{tr} \Big\{ \big(\operatorname{tr}_A\{\rho_{AB}^\alpha\}\big)^{\frac{1}{\alpha}} \Big\} \\ &= -\frac{1}{1-\beta} \log \operatorname{tr} \left\{ \left(\Big(1_A \otimes \rho_C^{\frac{1-\beta}{2\beta}}\Big) \rho_{AC} \Big(1_A \otimes \rho_C^{\frac{1-\beta}{2\beta}}\Big) \right)^\beta \right\} \\ &= \frac{\alpha}{1-\alpha} \log \operatorname{tr} \left\{ \left(\Big(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\Big) \rho_{AC} \Big(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\Big) \right)^{\frac{1}{\alpha}} \right\}, \end{aligned}$$

or, equivalently, that the operators

$$\operatorname{tr}_A\{\rho_{AB}^\alpha\} \qquad \text{and} \qquad \Big(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\Big) \rho_{AC} \Big(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\Big)$$

have the same spectrum of eigenvalues. To see that the latter statement is indeed true, note that both operators are marginals of the same tripartite rank-1 operator. More precisely, the first operator may be rewritten as

$$\begin{aligned}\mathrm{tr}_A\{\rho_{AB}^{\alpha}\} &= \mathrm{tr}_A\left\{\rho_{AB}^{\frac{\alpha-1}{2}}\,\rho_{AB}\,\rho_{AB}^{\frac{\alpha-1}{2}}\right\}\\ &= \mathrm{tr}_{AC}\left\{\left(\rho_{AB}^{\frac{\alpha-1}{2}}\otimes 1_C\right)\rho_{ABC}\left(\rho_{AB}^{\frac{\alpha-1}{2}}\otimes 1_C\right)\right\}\\ &= \mathrm{tr}_{AC}\left\{\left(1_{AB}\otimes\rho_C^{\frac{\alpha-1}{2}}\right)\rho_{ABC}\left(1_{AB}\otimes\rho_C^{\frac{\alpha-1}{2}}\right)\right\}.\end{aligned}$$

The spectra are thus equivalent, concluding the proof. □

The relation can readily be extended for all $\alpha \geq 0$ and $\beta > 0$. The limiting case $\alpha = 1$ is simply the duality of the conditional von Neumann entropy (16), whereas the case $\alpha = 0, \beta = \infty$ was shown in [8, Prop. 3.11]. (See also [37, Lm. 25] for a concise proof.)

Finally, note that the transformation $\alpha \mapsto \beta = \frac{1}{\alpha}$ maps the interval $[0, 2]$ where data-processing holds for $H_\alpha^{\uparrow}$ to $[\frac{1}{2}, \infty]$ where data-processing holds for $\widetilde{H}_\beta^{\downarrow}$.

We summarize these duality relations in the following theorem, where we take note that the first and second statements have been shown in [36] and [6], [29], respectively.

Theorem 3. *For any pure $\rho_{ABC} \in \mathcal{S}(ABC)$, the following duality relations hold:*[5]

$$H_\alpha^{\downarrow}(A|B)_\rho + H_\beta^{\downarrow}(A|C)_\rho = 0 \quad \textit{for } \alpha,\beta \in [0,2],\ \alpha+\beta = 2.$$

$$\widetilde{H}_\alpha^{\uparrow}(A|B)_\rho + \widetilde{H}_\beta^{\uparrow}(A|C)_\rho = 0 \quad \textit{for } \alpha,\beta \in \left[\frac{1}{2},\infty\right],\ \frac{1}{\alpha}+\frac{1}{\beta} = 2,$$

$$H_\alpha^{\uparrow}(A|B)_\rho + \widetilde{H}_\beta^{\downarrow}(A|C)_\rho = 0 \quad \textit{for } \alpha \in [0,\infty),\ \beta \in (0,\infty],\ \alpha\cdot\beta = 1.$$

IV. Inequalities Relating Conditional Entropies

Recently, Mosonyi [25, Lm. 2.1] used a converse of the Araki-Lieb-Thirring trace inequality due to Audenaert [3] to find a converse to the ordering relation $D_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\rho\|\sigma)$. Here we follow a different approach and show that inequalities of a similar type for the conditional entropies are a direct corollary of the duality relations in Theorem 3.

Corollary 4. *Let $\rho_{AB} \in \mathcal{S}(AB)$. Then, the following holds:*

$$H_\alpha^{\uparrow}(A|B)_\rho \leq \widetilde{H}_\alpha^{\uparrow}(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^{\uparrow}(A|B)_\rho \quad \textit{for } \alpha \in \left[\frac{1}{2},\infty\right], \tag{20}$$

$$H_\alpha^{\downarrow}(A|B)_\rho \leq H_\alpha^{\uparrow}(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^{\downarrow}(A|B)_\rho \quad \textit{for } \alpha \in \left[\frac{1}{2},\infty\right), \tag{21}$$

$$\widetilde{H}_\alpha^{\downarrow}(A|B)_\rho \leq \widetilde{H}_\alpha^{\uparrow}(A|B)_\rho \leq \widetilde{H}_{2-\frac{1}{\alpha}}^{\downarrow}(A|B)_\rho \quad \textit{for } \alpha \in \left(\frac{1}{2},\infty\right], \tag{22}$$

$$H_\alpha^{\downarrow}(A|B)_\rho \leq \widetilde{H}_\alpha^{\downarrow}(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^{\downarrow}(A|B)_\rho \quad \textit{for } \alpha \in \left[\frac{1}{2},\infty\right]. \tag{23}$$

[5] We use the convention that $\frac{1}{\infty} = 0$ and $0\cdot\infty = 1$ for ease of presentation.

Proof. Note that the first inequality on each line follows directly from the relations depicted in Figure 1. Next, consider an arbitrary purification $\rho_{ABC} \in \mathcal{S}(ABC)$ of ρ_{AB}. The relations of Figure 1, for any $\gamma \geq 0$, applied to the marginal ρ_{AC} are given as

$$\widetilde{H}_\gamma^{\uparrow}(A|C)_\rho \geq \widetilde{H}_\gamma^{\downarrow}(A|C)_\rho \geq H_\gamma^{\downarrow}(A|C)_\rho\,, \qquad \text{and}$$
$$\widetilde{H}_\gamma^{\uparrow}(A|C)_\rho \geq H_\gamma^{\uparrow}(A|C)_\rho \geq H_\gamma^{\downarrow}(A|C)_\rho\,.$$

We then substitute the corresponding dual entropies according to Theorem 3, which yields the desired inequalities upon appropriate new parametrization. □

We note that the fully classical (commutative) case of all these inequalities is trivial except for the second inequalities in (21) and (22), which were proven before by one of authors [19, Lm. 6]. Other special cases of these inequalities are also well known and have operational significance. For example, (22) for $\alpha = \infty$ states that $\widetilde{H}_\infty^{\uparrow}(A|B)_\rho \leq \widetilde{H}_2^{\downarrow}(A|B)_\rho$, which relates the conditional min-entropy in (12) to the conditional collision entropy in (13). To understand this inequality more operationally we rewrite the conditional min-entropy as its dual semi-definite program [23],

$$\widetilde{H}_\infty^{\uparrow}(A|B)_\rho = \inf_{\Lambda_{B\to A'}} -\log\left(|A|\cdot F(\Phi_{AA'},\Lambda_{B\to A'}[\rho_{AB}]\right),$$

where A' is a copy of A, the infimum is over all quantum channels $\Lambda_{B\to A'}$, $|A|$ denotes the dimension of A, and $\Phi_{AA'}$ is the maximally entangled state on AA'. Now, the above inequality becomes apparent since the conditional collision entropy can be written as [9],

$$\widetilde{H}_2^{\downarrow}(A|B)_\rho = -\log\left(|A|\cdot F(\Phi_{AA'},\Lambda^{\mathrm{pg}}_{B\to A'}[\rho_{AB}]\right),$$

where $\Lambda^{\mathrm{pg}}_{B\to A'}$ denotes the pretty good recovery map of Barnum and Knill [5]. Also, (20) for $\alpha = \frac{1}{2}$ yields $\widetilde{H}_{1/2}^{\uparrow}(A|B)_\rho \leq H_0^{\uparrow}(A|B)_\rho$, which relates the quantum conditional max-entropy in (14) to the quantum conditional generalization of the Hartley entropy in (15).

We believe that the sandwich relations (20)–(23) for α close to 1 will prove useful in applications in quantum information processing as they allow to switch between different definitions of the conditional Rényi entropy.

Acknowledgements: We thank Mark M. Wilde for pointing us to Ref. [15]. MT and MH acknowledge funding from the Ministry of Education (MOE) and National Research Foundation Singapore. MT is also funded MOE Tier 3 Grant "Random numbers from quantum processes" (MOE2012-T3-1-009). MB thanks the Center for Quantum Technologies, Singapore, for hosting him while this work was done. MH is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071 and the National Institute of Information and Communication Technology (NICT), Japan.

Appendix

We prove the following Hölder and reverse Hölder inequalities for traces of operators. (See also [21, Appendix A] and references given there.)

Lemma 5. *Let $A, B \geq 0$ and let $p > 0$, $q \in \mathbb{R}$ such that $\frac{1}{p} + \frac{1}{q} = 1$. Then, the following Hölder and reverse Hölder inequalities hold:*

$$\operatorname{tr}\{AB\} \leq \big(\operatorname{tr}\{A^p\}\big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \quad \text{if } p > 1\,, \tag{24}$$

$$\operatorname{tr}\{AB\} \geq \big(\operatorname{tr}\{A^p\}\big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \quad \text{if } p < 1 \text{ and } B \gg A\,. \tag{25}$$

Here, B^q is evaluated on the support of B by convention.

The first statement also immediately follows from a Hölder inequality for unitarily invariant norms (the trace norm in this case), e.g. in [10, Cor. IV.2.6]. The following proof is a simple reduction to the classical case.

Proof. For commuting A and B, the above result immediately follows from the corresponding classical Hölder and reverse Hölder inequalities. Now, let $\mathcal{M}$ be a pinching in the eigenbasis of B. Since $\operatorname{tr}\{AB\} = \operatorname{tr}\{\mathcal{M}[A]B\}$, we thus have

$$\operatorname{tr}\{AB\} \leq \Big(\operatorname{tr}\Big\{\big(\mathcal{M}[A]\big)^p\Big\}\Big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \qquad \text{if } p > 1,$$

$$\operatorname{tr}\{AB\} \geq \Big(\operatorname{tr}\Big\{\big(\mathcal{M}[A]\big)^p\Big\}\Big)^{\frac{1}{p}} \big(\operatorname{tr}\{B^q\}\big)^{\frac{1}{q}} \qquad \text{if } p < 1\,.$$

under the respective constraints. Now, note that for $p > 1$, we have $\|\mathcal{M}[A]\|_p \leq \|A\|_p$ by the pinching inequality for the Schatten p-norm [10, Eq. (IV.52)] and (24) follows. On the other hand, for $p < 1$, we use [10, Thm. V.2.1], which implies that $\big(\mathcal{M}[A]\big)^p \geq \mathcal{M}[A^p]$. This yields (25) and concludes the proof. □

References

[1] H. Araki. On an inequality of Lieb and Thirring. *Lett. Math. Phys.*, 19(2):167–170, Feb. 1990.

[2] S. Arimoto. Information Measures and Capacity of Order alpha for Discrete Memoryless Channels. *Colloq. Math. Soc. János Bolya*, 16:41–52, 1975.

[3] K. M. R. Audenaert. On the Araki-Lieb-Thirring Inequality. *Int. J. Inf. Syst. Sci.*, 4(1):78–83, Jan. 2008. arXiv: math/0701129.

[4] K. M. R. Audenaert and N. Datta. α-z-relative Renyi entropies. Oct. 2013. arXiv: 1310.7178.

[5] H. Barnum and E. Knill. Reversing Quantum Dynamics with Near-Optimal Quantum and Classical Fidelity. *J. Math. Phys.*, 43(5):2097, 2002.

[6] S. Beigi. Quantum Rényi Divergence Satisfies Data Processing Inequality. June 2013. arXiv: 1306.5920.

[7] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized Privacy Amplification. *IEEE Trans. Inf. Theory*, 41(6):1915–1923, 1995.

[8] M. Berta. Single-Shot Quantum State Merging. Master's thesis, ETH Zurich, 2008. arXiv: 0912.4495.

[9] M. Berta, P. J. Coles, and S. Wehner. An equality between entanglement and uncertainty. page 5, Feb. 2013. arXiv: 1302.5902.

[10] R. Bhatia. *Matrix Analysis*. Graduate Texts in Mathematics. Springer, 1997.

[11] I. Csiszár. Generalized Cutoff Rates and Renyi's Information Measures. *IEEE Trans. Inf. Theory*, 41(1):26–34, 1995.

[12] N. Datta and F. Leditzky. A Limit of the Quantum Renyi Divergence. Aug. 2013. arXiv: 1308.5961.

[13] R. L. Frank and E. H. Lieb. Monotonicity of a relative Rényi entropy. June 2013. arXiv: 1306.5358.

[14] R. G. Gallager. Source Coding with Side Information and Universal Coding. In *Proc. IEEE ISIT*, volume 21, Ronneby, Sweden,, June 1979. IEEE.

[15] M. K. Gupta and M. M. Wilde. Multiplicativity of Completely Bounded p-Norms Implies a Strong Converse for Entanglement-Assisted Capacity. Oct. 2013. arXiv: 1310.7028.

[16] R. V. L. Hartley. Transmission of Information. *Bell Syst. Tech. J.*, 7(3):535–563, July 1928.

[17] M. Hayashi. Exponential Decreasing Rate of Leaked Information in Universal Random Privacy Amplification. *IEEE Trans. Inf. Theory*, 57(6):3989–4001, June 2011.

[18] M. Hayashi. Large Deviation Analysis for Quantum Security via Smoothing of Renyi Entropy of Order 2. Feb. 2012. arXiv: 1202.0322.

[19] M. Hayashi. Security Analysis of epsilon-Almost Dual Two-Universal Hash Functions. Sept. 2013. arXiv: 1309.1596.

[20] M. Hayashi. Tight Exponential Analysis of Universally Composable Privacy Amplification and Its Applications. *IEEE Trans. Inf. Theory*, 59(11):7728–7746, Nov. 2013.

[21] F. Hiai, M. Mosonyi, D. Petz, and C. Bény. Quantum f-Divergences and Error Correction. *Rev. Math. Phys.*, 23(07):691–747, Aug. 2011.

[22] M. Iwamoto and J. Shikata. Information Theoretic Security for Encryption Based on Conditional Renyi Entropies. 2013. Available online: http://eprint.iacr.org/2013/440.

[23] R. König, R. Renner, and C. Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. Inf. Theory*, 55(9):4337–4347, Sept. 2009.

[24] E. H. Lieb and W. E. Thirring. Inequalities for the Moments of the Eigenvalues of the Schrödinger Hamiltonian and Their Relation to Sobolev Inequalities. In *Stab. Matter From Atoms to Stars*, chapter III, pages 205–239. Springer Berlin Heidelberg, 2005.

[25] M. Mosonyi. Rényi Divergences and the Classical Capacity of Finite Compound Channels. 2013. arXiv: 1310.7525.

[26] M. Mosonyi and F. Hiai. On the Quantum Rényi Relative Entropies and Related Capacity Formulas. *IEEE Trans. Inf. Theory*, 57(4):2474–2487, Apr. 2011.

[27] M. Mosonyi and T. Ogawa. Quantum Hypothesis Testing and the Operational Interpretation of the Quantum Renyi Relative Entropies. Sept. 2013. arXiv: 1309.3228.

[28] M. Müller-Lennert. *Quantum Relative Rényi Entropies*. Master thesis, ETH Zurich, Apr. 2013.

[29] M. Muller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On Quantum Renyi Entropies: A new Generalization and Some Properties. *J. Math. Phys.*, 54(12):122203, June 2013.

[30] H. Nagaoka. The Converse Part of The Theorem for Quantum Hoeffding Bound. Nov. 2006. arXiv: quant-ph/0611289.

[31] T. Ogawa and M. Hayashi. On Error Exponents in Quantum Hypothesis Testing. *IEEE Trans. Inf. Theory*, 50(6):1368–1372, June 2004.

[32] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, Dec. 2005. arXiv: quant-ph/0512258.

[33] A. Rényi. On Measures of Information and Entropy. In *Proc. Symp. Math., Stat. Probab.*, pages 547–561, Berkeley, 1961. University of California Press.

[34] N. Sharma and N. A. Warsi. Fundamental Bound on the Reliability of Quantum Information Transmission. *Phys. Rev. Lett.*, 110(8):080501, Feb. 2013.

[35] M. Tomamichel. Smooth entropies—A tutorial: With focus on applications in cryptography, Sept. 2012. Available online: http://2012.qcrypt.net/docs/slides/Marco.pdf.

[36] M. Tomamichel, R. Colbeck, and R. Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Trans. Inf. Theory*, 55(12):5840–5847, Dec. 2009.

[37] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover Hashing Against Quantum Side Information. *IEEE Trans. Inf. Theory*, 57(8):5524–5535, Aug. 2011.

[38] M. M. Wilde, A. Winter, and D. Yang. Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels. June 2013. arXiv: 1306.1586.

[39] H. Yagi. Finite Blocklength Bounds for Multiple Access Channels with Correlated Sources. In *Proc. IEEE ISITA*, pages 377–381, 2012.